

The Role of PKI and Electronic Signatures in eGovernment



We Make Paperless Happen™

State of Kansas PKI Education Day
November 3rd, 2005

*Robert Al-Jaar, PhD
Chief Technology Officer*

Three Things to Walk Away With

- I. Electronic signatures are the missing link to paperless processes
- II. Approval automation is a public key-enabled application
- III. Selection of eAuthentication method depends on the level of acceptable risk

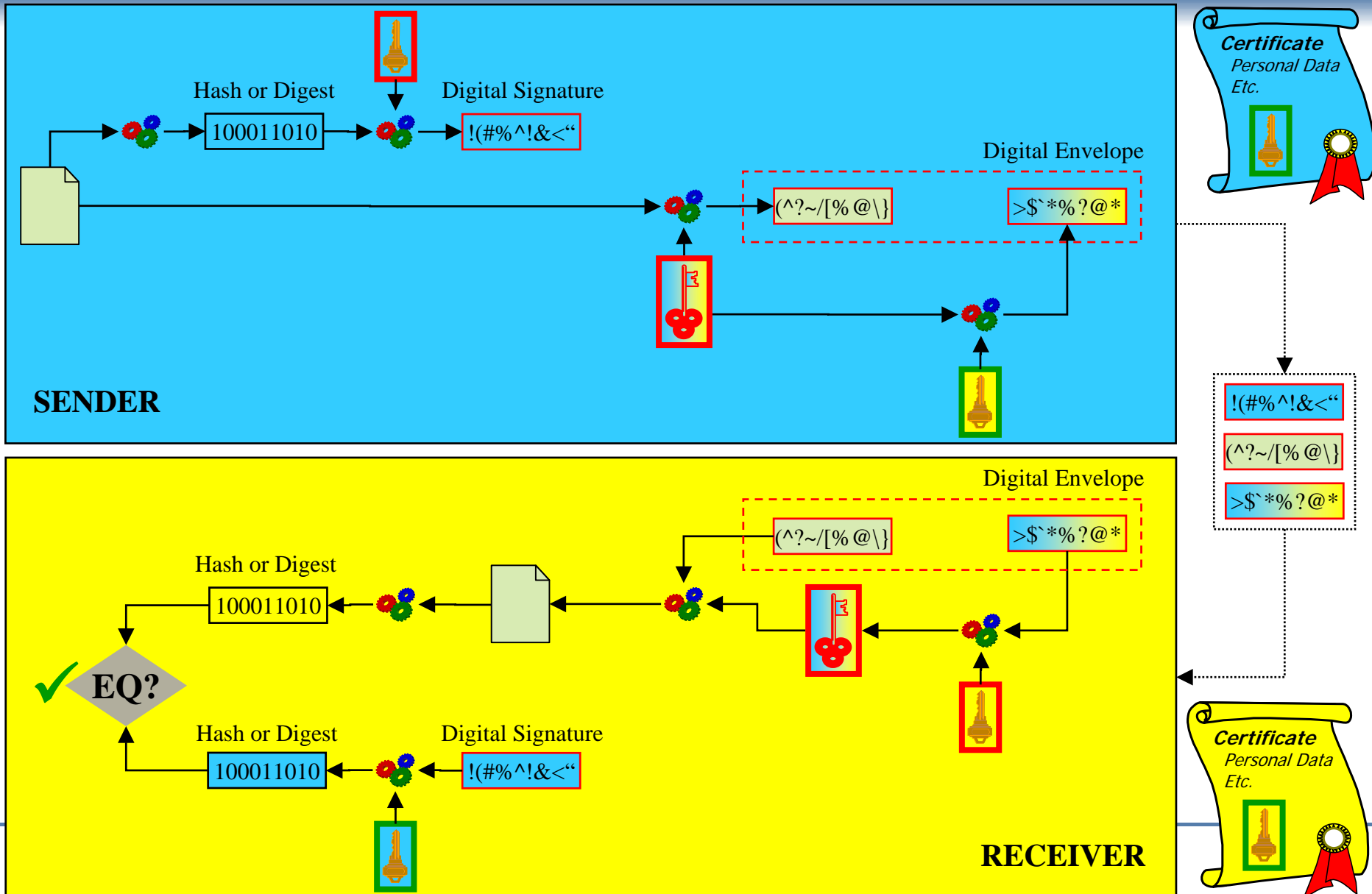


- ② Overview of PKI and PKE
- ② Electronic Signatures, an eGov Imperative
- ② Key Concepts and Terminology
- ② The Electronic Approval Process
 - Capturing intent & consent
 - Why digital signatures are not enough
- ② eAuthentication
- ② Risk Assessment
- ② Examples of Electronic Signature Initiatives
- ② Conclusion

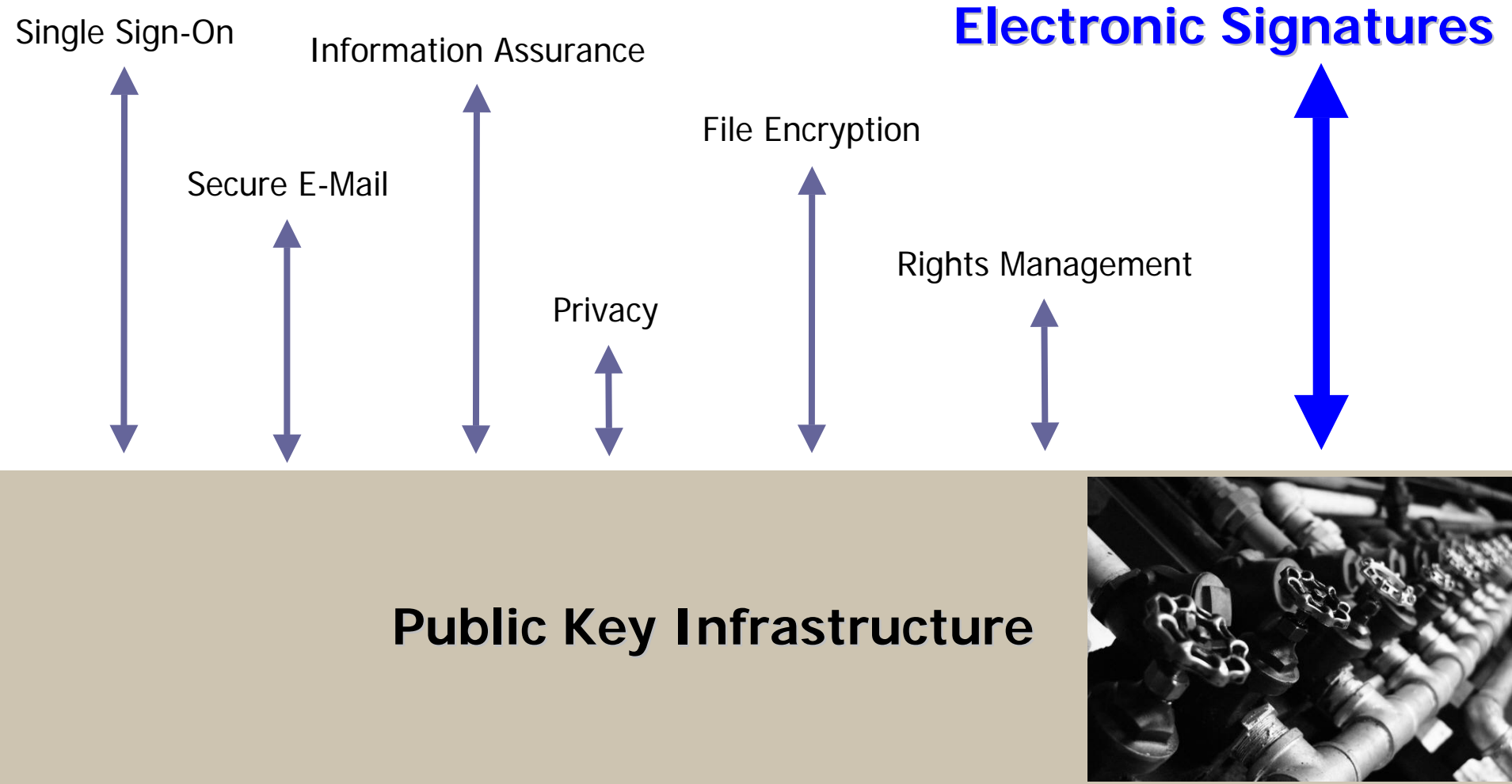
- ② **Overview of PKI and PKE**
- ② Electronic Signatures, an eGov Imperative
- ② Key Concepts and Terminology
- ② The Electronic Approval Process
 - Capturing intent & consent
 - Why digital signatures are not enough
- ② eAuthentication
- ② Risk Assessment
- ② Examples of Electronic Signature Initiatives
- ② Conclusion

Brief Overview of PKI

D. Hiley



PKE Applications



- ② Overview of PKI and PKE
- ② **Electronic Signatures, an eGov Imperative**
- ② Key Concepts and Terminology
- ② The Electronic Approval Process
 - Capturing intent & consent
 - Why digital signatures are not enough
- ② eAuthentication
- ② Risk Assessment
- ② Examples of Electronic Signature Initiatives
- ② Conclusion

Totally Electronic Business Processes

The Last Step: Eliminate Paper Signatures

Regulation, Legislation, Policy-Driven Requirements

The end-to-end “approval” process consists of many steps:

- Create and Prepare
- Authenticate
- Present and Review
- Sign
- Route and Validate
- Deliver
- Vault
- Scan and Retain
- Prove unique “original”
- Manage Authoritative Copy
- Audit and Accounting
- Manage and Administer

SECURITY

The Significance of Approvals



- Organizations run on **decisions**
- Approvals **capture** these decisions
- Electronic signatures allow you to easily **audit** or **track** these decisions
- This is critical to ensuring and enforcing **compliance**

REGULATION

- *FDA*
- *FAA*
- *OMB*
- *HIPAA*
- *FTC*



LEGISLATION

- *Graham-Leach Bliley*
- *US Patriot Act*
- *Sarbanes-Oxley*



POLICY

- *ISO*
- *Six Sigma*
- *MISMO*
- *ACORD*



Value of Approval Automation



Citizen Experience

- ② Improve service delivery
- ② Simplify interactions with citizens
- ② Increase responsiveness



Operational Efficiency

- ② Streamline processes
- ② Eliminate unnecessary costs



External Interactions

- ② Increase efficiency in contractor relationships

Different Functions, Different Concerns

D. Ashley



Business impact, legality, auditability

Process Owner
(Business Perspective)



Integration, customization, standards

Application Developer
(Information Technology)



Deployment, scalability, support

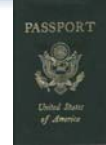
Operations Manager
(Data Center)

- ② Overview of PKI and PKE
- ② Electronic Signatures, an eGov Imperative
- ② **Key Concepts and Terminology**
- ② The Electronic Approval Process
 - Capturing intent & consent
 - Why digital signatures are not enough
- ② eAuthentication
- ② Risk Assessment
- ② Examples of Electronic Signature Initiatives
- ② Conclusion

"eSigning" Concepts



- ② **Digital Certificate** = Electronic ID
- ② **Certificate Authority (CA)** = Trusted third party who takes responsibility for identifying and issuing electronic IDs
- ② **PKI** = A secure system that manages Digital Certificates and cryptographic keys
- ② **Digital Signature** = Encryption process using private keys (to "sign") and public keys (to verify)
 - It is NOT the electronic equivalent of a paper signature
- ② **Electronic Signature** = A legal concept, "any sound, symbol, mark, or process" used to capture intent & consent

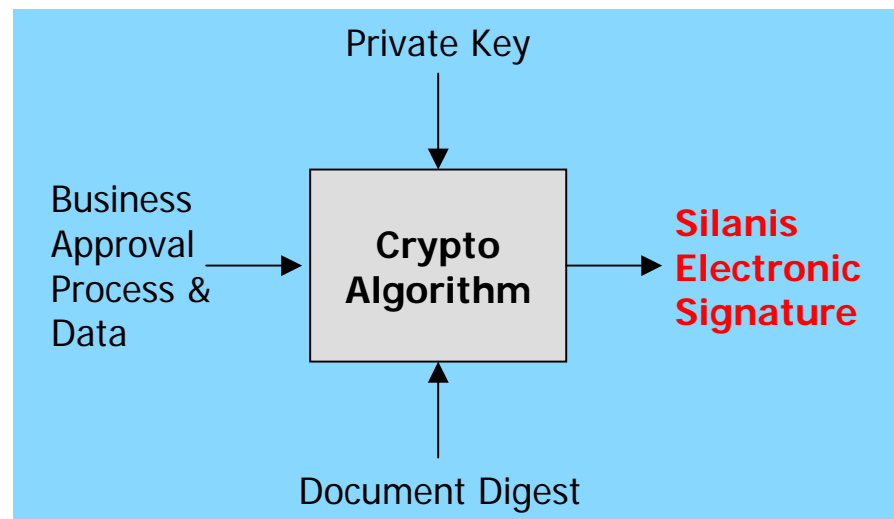
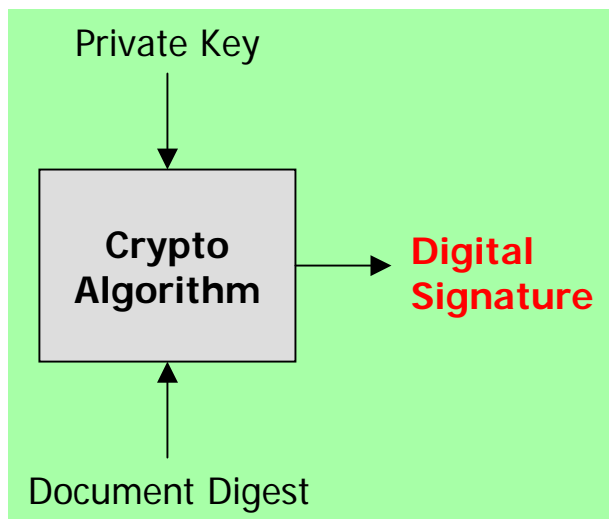


The Silanis Electronic Signature Defined



**The Silanis Electronic Signature =
Digital Signature + Business Approval Process & Data**

- ② PKE application that uses PKI and digital signature technologies
- ② Extends digital signatures to address requirements of real-world business approval processes

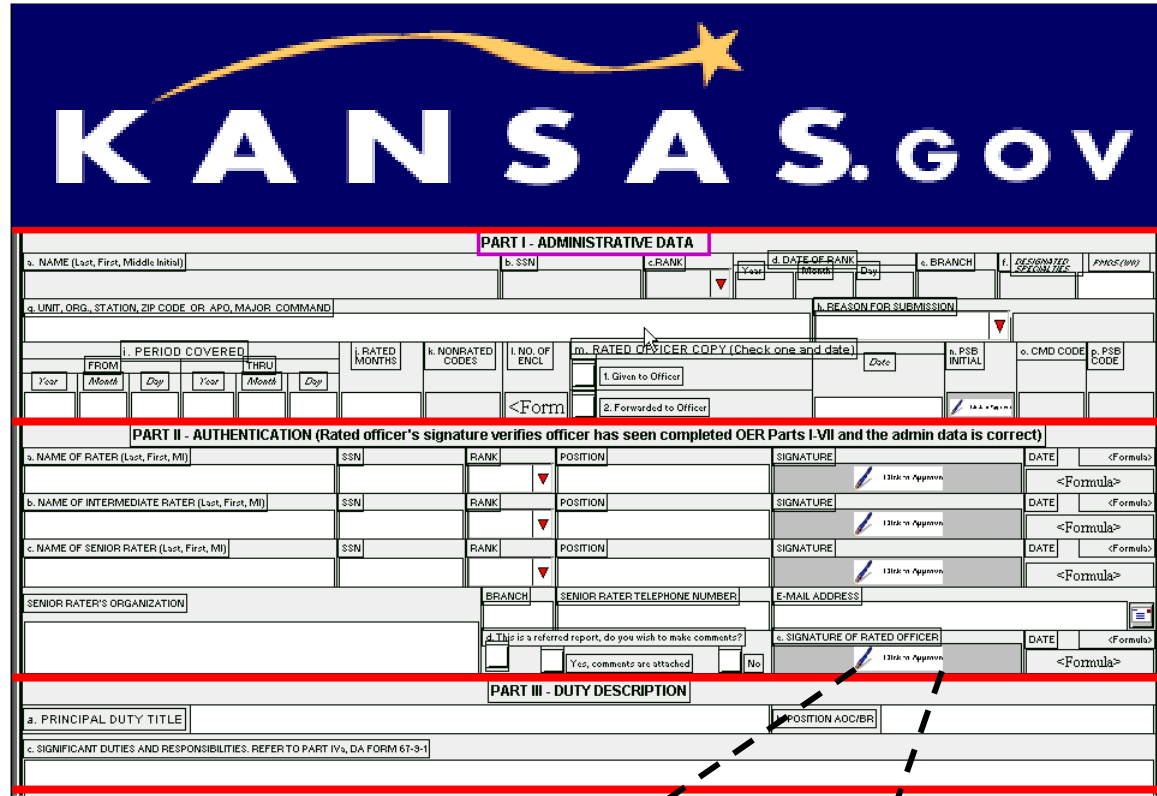


- ② Overview of PKI and PKE
- ② Electronic Signatures, an eGov Imperative
- ② Key Concepts and Terminology
- ② **The Electronic Approval Process**
 - **Capturing intent & consent**
 - **Why digital signatures are not enough**
- ② eAuthentication
- ② Risk Assessment
- ② Examples of Electronic Signature Initiatives
- ② Conclusion

The eApproval Process – Prepare & Review



- Templates to Select Data for Signing
- Sectional Signing
- Multiple Signers
- Hierarchical Approval Chain
- Signature Blocks



KANSAS.GOV

PART I - ADMINISTRATIVE DATA

a. NAME (Last, First, Middle Initial) b. SSN c. RANK d. DATE OF BIRTH e. BRANCH f. DESIGNATED OFFICIAL g. PMOS (MOS)

h. UNIT, ORG., STATION, ZIP CODE OR APO, MAJOR COMMAND i. REASON FOR SUBMISSION

j. PERIOD COVERED k. RATED MONTHS l. NONRATED CODES m. RATED OFFICER COPY (Check one and date)

1. Given to Officer 2. Forwarded to Officer

PART II - AUTHENTICATION (Rated officer's signature verifies officer has seen completed OER Parts I-VII and the admin data is correct)

a. NAME OF RATER (Last, First, MI) b. SSN c. RANK d. POSITION e. SIGNATURE f. DATE (Formula)

b. NAME OF INTERMEDIATE RATER (Last, First, MI) b. SSN c. RANK d. POSITION e. SIGNATURE f. DATE (Formula)

c. NAME OF SENIOR RATER (Last, First, MI) b. SSN c. RANK d. POSITION e. SIGNATURE f. DATE (Formula)

SENIOR RATER'S ORGANIZATION BRANCH SENIOR RATER TELEPHONE NUMBER E-MAIL ADDRESS

d. This is a referred report, do you wish to make comments? Yes, comments are attached No e. SIGNATURE OF RATED OFFICER f. DATE (Formula)

PART III - DUTY DESCRIPTION

a. PRINCIPAL DUTY TITLE b. POSITION AOC/BR

c. SIGNIFICANT DUTIES AND RESPONSIBILITIES. REFER TO PART IV, DA FORM 61-3-1



Click to Approve

The eApproval Process – Sign



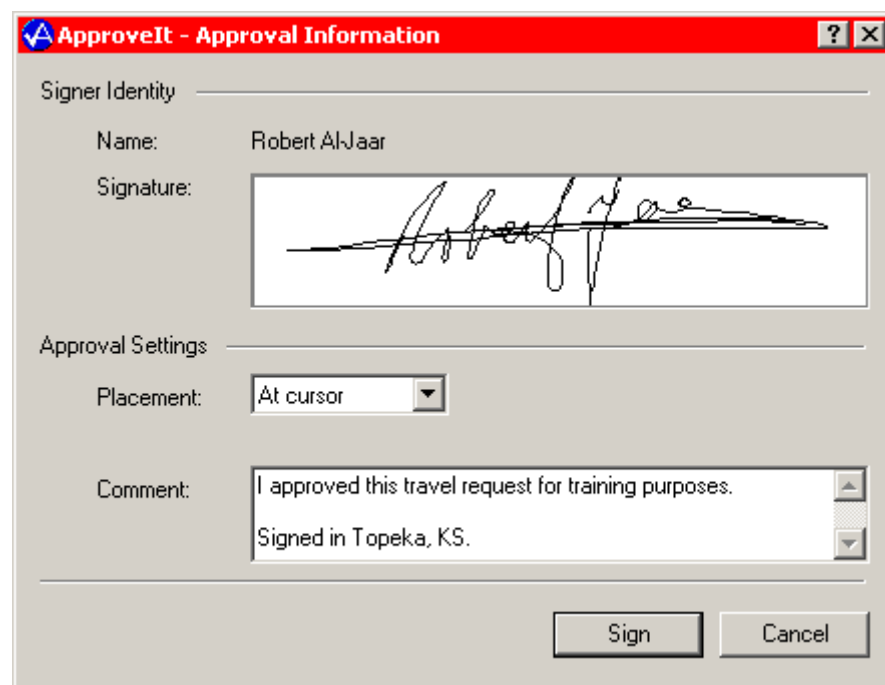
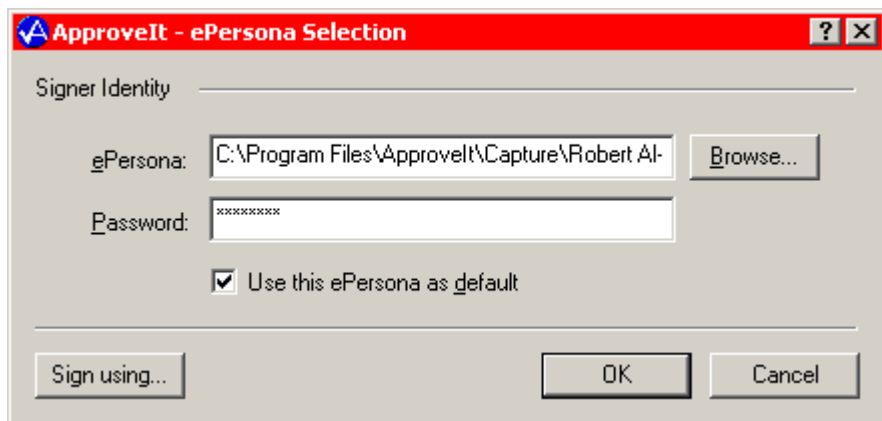
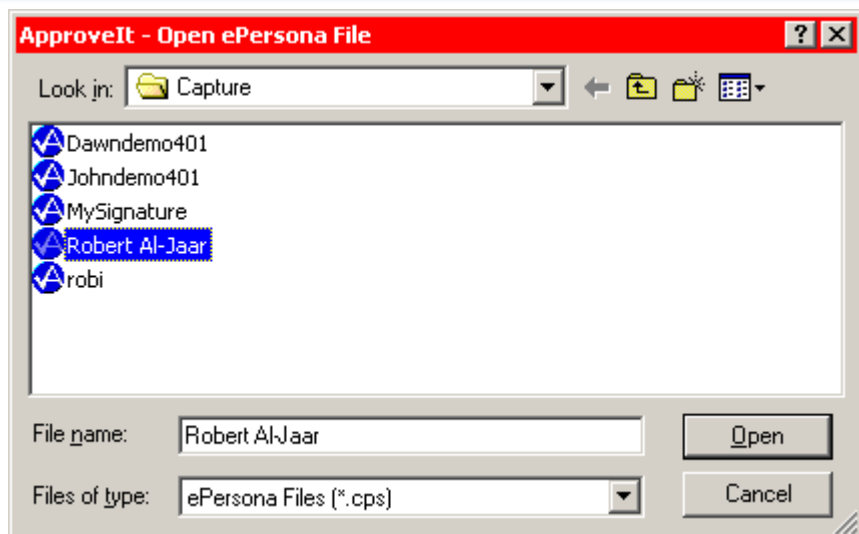
- ② Digitized Signatures
- ② Automatic Signer's Information
 - Smart Cards, Soft Certificates
- ② Trusted Timestamps
- ② Certificate Validation
 - CML, CRL, OCSP, LDAP, CAM
- ② Signing Ceremony
 - Capture **intent** and **consent**



Capturing Intent and Consent - Internal



Rich-Client, Desktop Application



Capturing Intent and Consent - External



Zero-Client, Web Application

Electronic Review and Signing Process

[E-Signature
Information](#)

[FAQ](#)

[HELP](#)

[Contact](#)

[Sample
Signature
Process
Signature](#)

Origination Documents

3 documents

<input type="checkbox"/>	E-Sign Consent	Not Accepted
<input type="checkbox"/>	Government Disclosures	Not Accepted
<input type="checkbox"/>	Uniform Residential Loan Application	Not Signed

Closing / Title Documents

4 documents

<input type="checkbox"/>	E-Sign Consent	Not Accepted
<input type="checkbox"/>	Truth In Lending Disclosure	Not Signed
<input type="checkbox"/>	Deed of Trust	Not Signed
<input type="checkbox"/>	Note	Not Signed

Preview & Print Selected



[Cancel](#)

[Save & Exit](#)

[Submit >](#)

We Make Paperless Happen™

© Silanis 2005 – Proprietary & Confidential – For use by the Government of Kansas only

The eApproval Process – Audit and Verify

D. Hiley

- » Confirm Signer's Identity
- » Confirm Signing Certificate Validity
- » Indicate Signature Status
 - Valid
 - Invalid
 - Revalidated


ApproveIt - Audit Trail - 3 signatures - 3 signature blocks

This document has been modified and revalidated.

Date & Time	Signed by	User Name	Revalidated by
Sunday, 17 October, 2004 22:10:04	Frodo Baggins	EIM-AGM04	Beef Cake
Sunday, 17 October, 2004 22:11:08	Beef Cake	EIM-AGM04	
Sunday, 17 October, 2004 22:11:36	John Hancock	EIM-AGM04	

Signing Information | Authentication | Replaced Fields | Advanced

Comment: I have modified the Executive Summary and re-approved the document in Washington DC.

Signature:  ✓

Certificate: **Certificate is revoked.** [Show Details...](#)




ApproveIt - Certificate Information

Owner: CAKE.BEEF.8.1160094334
Issued by: DOD CLASS 3 OM CA-10

Certificate Validity

☐ At signing time (10/17/2004) ☒ Today

 Certificate has been revoked.

- ✓ Certificate is valid from 10/12/2004 to 10/12/2007.
- ✓ Certificate's issuer is trusted.
- ✗ Certificate has been revoked.

Method: OCSP
URL: <http://cms-fcmp05>
Reason: Certificate key compromised

Certificate Information

Field	Value
Version	v3
Serial number	1886D5
Issuer	C=US, O=U.S. Government, OU=DOD, OU=PKI, CN=...
Valid from	2004-10-13T00:00:00Z
Valid to	2007-10-12T23:59:59Z
Subject	C=US, O=U.S. Government, OU=DOD, OU=PKI, OU=...

[Close](#) [Help](#)

Why Digital Signatures Are Not Enough



	Digital Signature	Silanis eSignature
Authentication	✓	✓
Data Integrity	✓	✓
Non-Repudiation	✓	✓
Privacy	✓	✓
Auditability	Basic	Extensive
Legal Intent & Consent	✗	✓
Digitized Signature	✗	✓
Automated Signer Data	✗	✓
Sectional Signing	✗	✓
Multiple Signers	✗	✓
Embedded Signatures	✗	✓
Preserve Document Format	✗	✓
Secure Print	✗	✓
Visual Status Validation	✗	✓

- ② Overview of PKI and PKE
- ② Electronic Signatures, an eGov Imperative
- ② Key Concepts and Terminology
- ② The Electronic Approval Process
 - Capturing intent & consent
 - Why digital signatures are not enough
- ② **eAuthentication**
- ② Risk Assessment
- ② Examples of Electronic Signature Initiatives
- ② Conclusion

The Significance of User Authentication



- ② Confirms identity of a party to a transaction
- ② Minimizes repudiation of signed documents
- ② Detects and prevents fraud or unauthorized use

Identification and Authentication



- ② Identification
 - Who are you?
- ② Authentication
 - Prove it!
- ② Authentication Levels
 - “One-Factor”: Something you know
 - Name, PIN, mother’s maiden name
 - “Two-Factor”: Something you have
 - Smart card, hardware token
 - “Three-Factor”: Something you are
 - Voice, eyes, face, fingerprints
 - Also provides identification



- ② CA-Issued Digital Certificates
 - Backed by trusted issuance policies & procedures
- ② Self-Signed Digital Certificates
 - Similar to wet ink signatures in paper world
- ② Smart Cards
 - Increase portability of certificates without compromising security
- ② User ID & Password
 - Leverage history of trust with online users
- ② Real Time Signature
 - Equivalent to wet ink signatures in paper world
- ② Biometrics Technologies
 - High assurance user authentication

eSigning and Online User Authentication



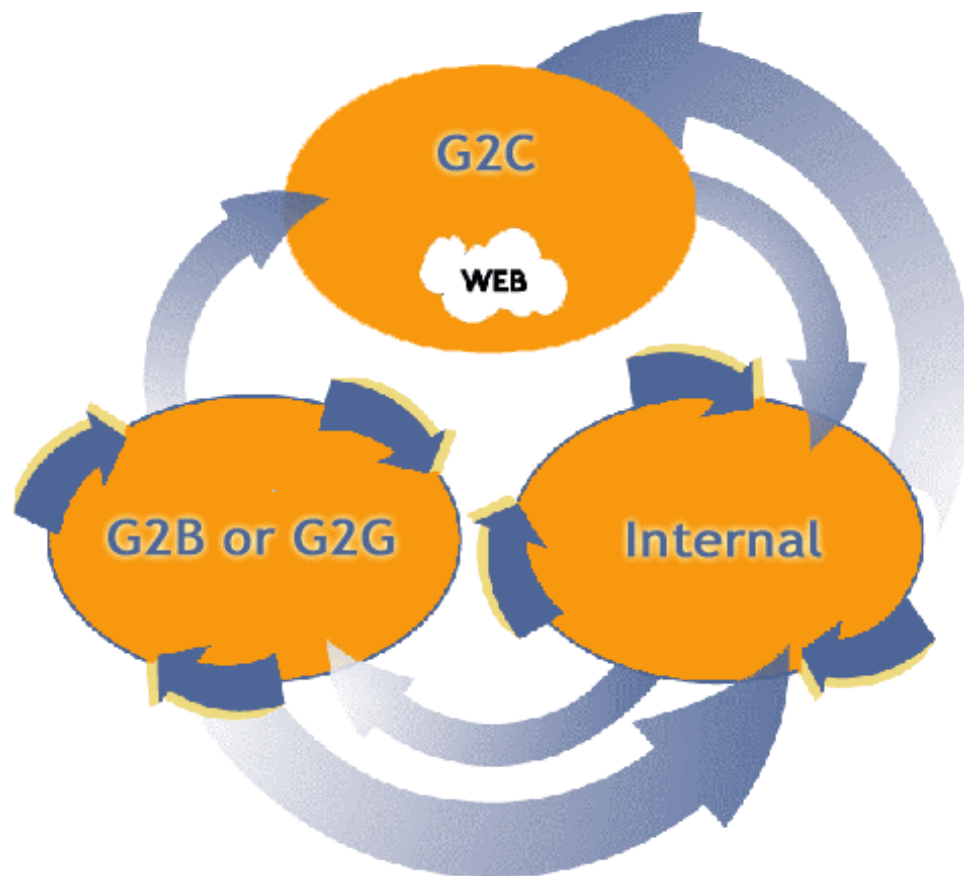
eSignature	User Authentication	Ideal for
Process Signature	PIN or Digital Certificate	Most online transactions, business processes
"I Agree" Button (Click-through)	PIN or mouse click only	Web-based standard agreements, proprietary systems
Real-Time Signatures	Identity verification	Point-of-sale, in-person transactions, processes
Biometric Device (fingerprint, voice, hand)	Included – may require login to template database for verification	High-risk processes with known & repeat users in controlled environments
Smart Card/Token	Included – may require login to access digital certificate for verification; may also require a CRL check	High-risk processes with known & repeat users in controlled environments

- ② Overview of PKI and PKE
- ② Electronic Signatures, an eGov Imperative
- ② Key Concepts and Terminology
- ② The Electronic Approval Process
 - Capturing intent & consent
 - Why digital signatures are not enough
- ② eAuthentication
- ② **Risk Assessment**
- ② Examples of Electronic Signature Initiatives
- ② Conclusion

Choosing the Right Approach

D. Hiley

KNOW YOUR BUSINESS PROCESS



Evaluating Risk Factors



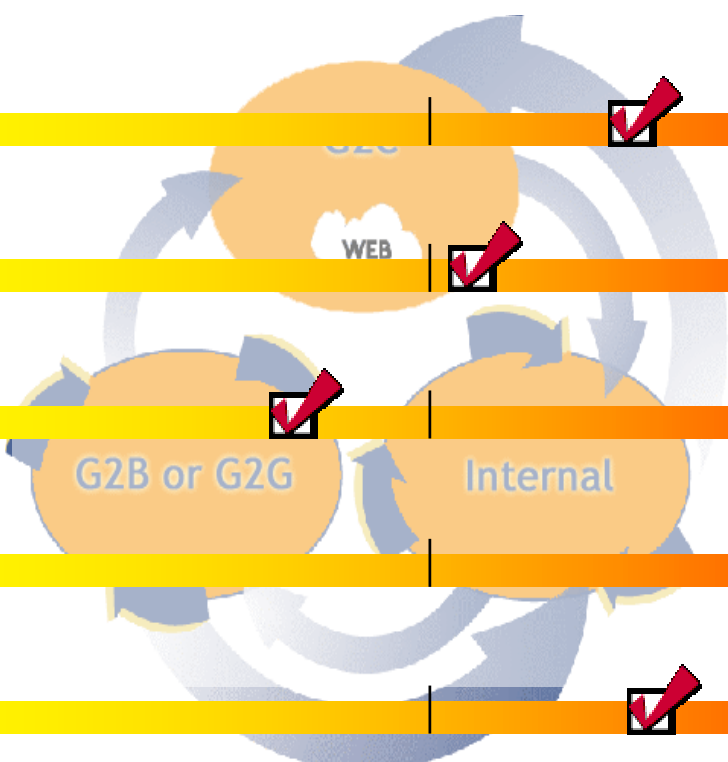
	Lower Risk	Mid Risk	Higher Risk
Frequency	Regular	Occasionally	One-Time
Location	In-Person	Online & Phone	Online
Value	Low	Mid	High
Signers	One	Few	Many
Relationship	Known	Casual	Unknown
Process Time	Weeks	Hours	Minutes
Type	Internal	Partners	External

Risk Assessment Example

D. Hiley

TIMESHEETS

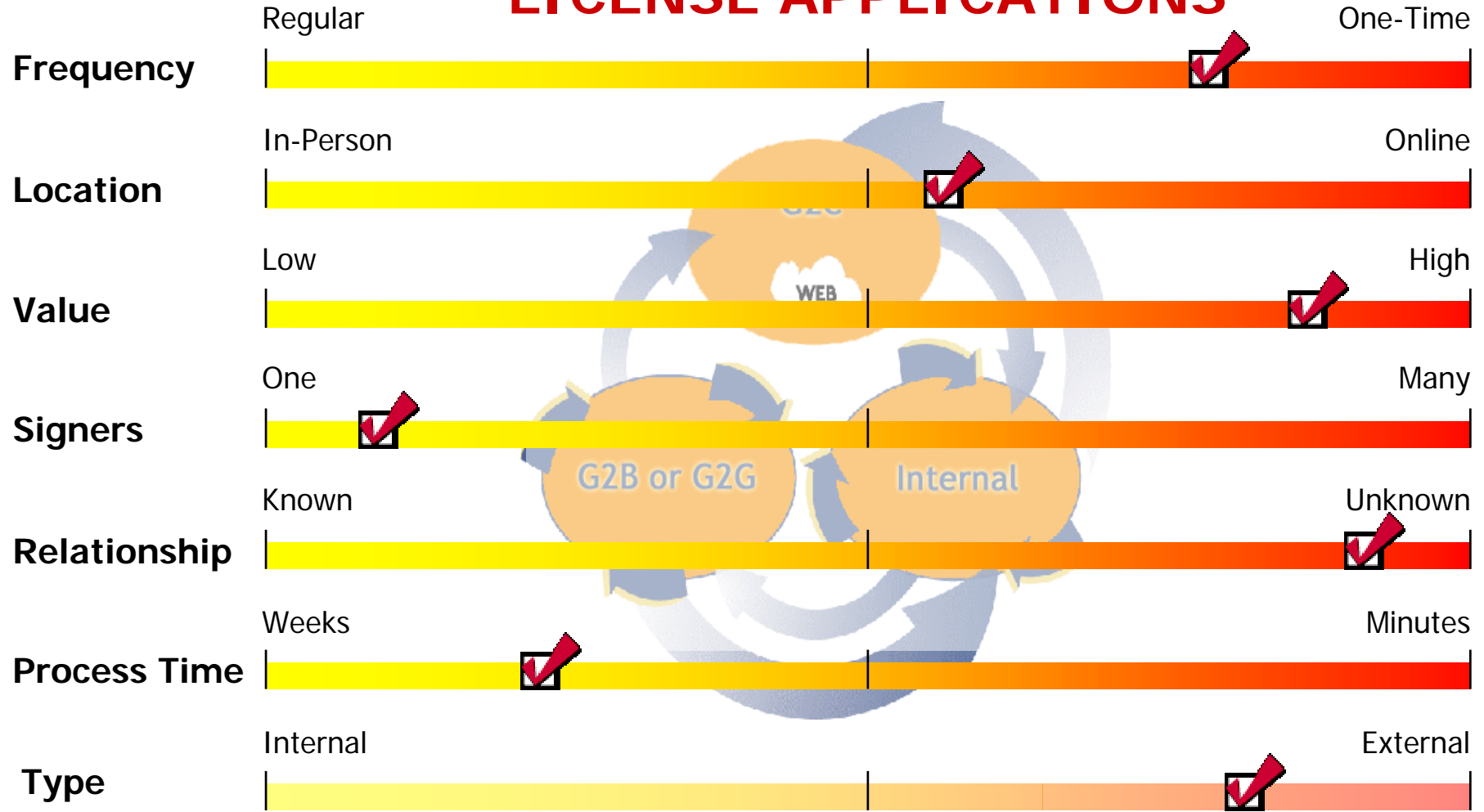
Frequency	Regular	One-Time
Location	In-Person	Online
Value	Low	High
Signers	One	Many
Relationship	Known	Unknown
Process Time	Weeks	Minutes
Type	Internal	External



Risk Assessment Example

D. Hiley

LICENSE APPLICATIONS



Choosing the Right Approach

D. Ashley



Usability



Security

- ② Overview of PKI and PKE
- ② Electronic Signatures, an eGov Imperative
- ② Key Concepts and Terminology
- ② The Electronic Approval Process
 - Capturing intent & consent
 - Why digital signatures are not enough
- ② eAuthentication
- ② Risk Assessment
- ② **Examples of Electronic Signature Initiatives**
- ② Conclusion

Deployed Electronic Signature Initiatives



Organization	eSignature Initiative
KDOT	<ul style="list-style-type: none">• Timesheets, Purchase Orders, HR Benefits• 1,000 users• ePersonas and self-signed certificates
Joint Chiefs of Staff	<ul style="list-style-type: none">• Sensitive Internal Processes, Joint Staff Action Processing• 1,500 users• ePersonas and self-signed certificates
State of Kentucky	<ul style="list-style-type: none">• Inspection Reports, Mining Permit Applications, Enforcement Actions, Vendor Invoices• 500 users• ePersonas and self-signed certificates
US Army G3	<ul style="list-style-type: none">• Ammunition Request Form including "troops in the field" (deployed units in Iraq)• 4,000 users, 150,000 HTML approvals per month• ePersonas and smart cards (DoD PKI)
GSA	<ul style="list-style-type: none">• New contractor enrollment and GSA schedule modifications• 13,000 contractors• User ID & password with Process signature (zero-client, Web-based environment)

Deployed Electronic Signature Initiatives



Organization	eSignature Initiative
Delaware Health and Social Services	<ul style="list-style-type: none">• Program Applications, Food Voucher Receipts, Lost/Stolen Voucher Reports• All clinics throughout State equipped with e-signing capability• Real-time signing with capture tablets
White Sands Missile Range	<ul style="list-style-type: none">• Operational Procedures, Daily Petroleum Report, Task Memorandums, Travel Orders• 1,200 users• ePersonas and smart cards (DoD PKI)
Army Recruiting	<ul style="list-style-type: none">• Recruitment application• 1,700 recruiting stations worldwide, 200,000 applications per year• Real-time signing with capture tablets
MEDCOM	<ul style="list-style-type: none">• Various medical records• 50,000 users• ePersonas and self-signed certificates

- ② Overview of PKI and PKE
- ② Electronic Signatures, an eGov Imperative
- ② Key Concepts and Terminology
- ② The Electronic Approval Process
 - Capturing intent & consent
 - Why digital signatures are not enough
- ② eAuthentication
- ② Risk Assessment
- ② Examples of Electronic Signature Initiatives
- ② **Conclusion**

Three Things to Walk Away With

- I. Electronic signatures are the missing link to paperless processes
- II. Approval automation is a public key-enabled application
- III. Selection of eAuthentication method depends on the level of acceptable risk



A Word about Silanis

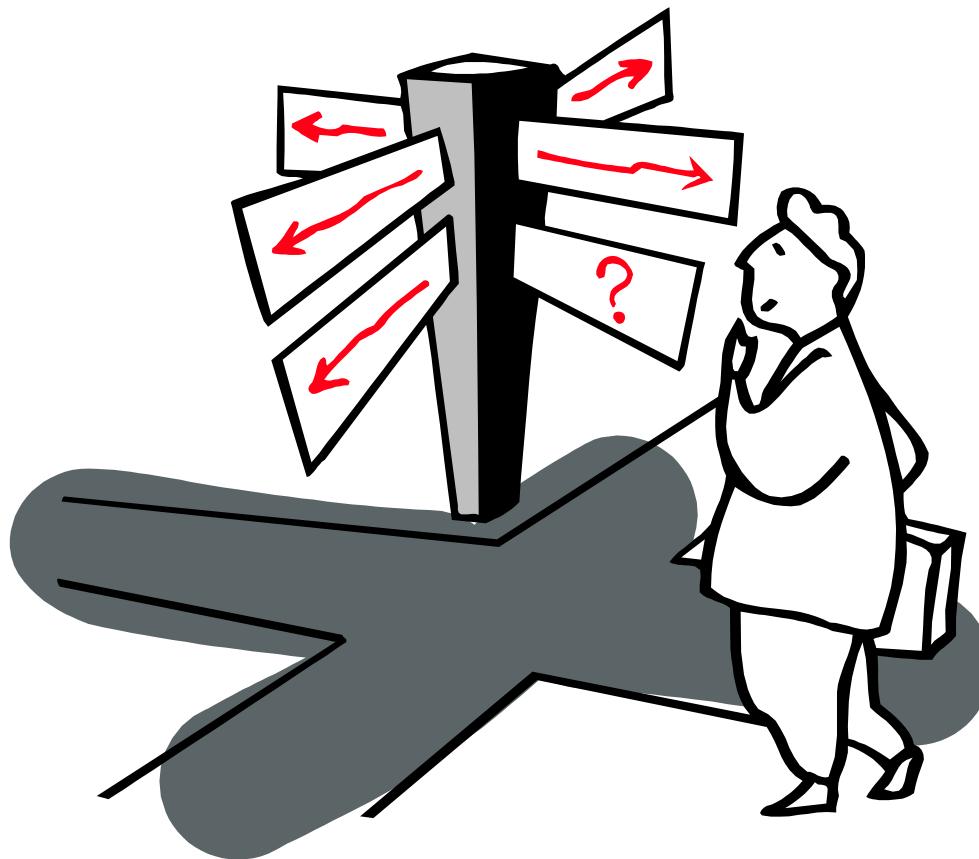


- Provider of eSignature, eDelivery and eVaulting solutions
- Over 2 million users and consumers in Government and Business using Silanis
- Experience in delivering enterprise level solutions... **Go-Live FAST™ !**
- Driving member in legal, regulatory, and standards organizations
- With Silanis, you can *Go Paperless* – today!

Silanis... **We Make Paperless Happen™**

For More Information...

D. Hiley



For Silanis e-Signature Resource Center
www.silanis.com/site/resource_center

Thank you for your time